Appendix B
Answers to Written Labs

Chapter 1: Security Governance Through Principles and Policies

1. The CIA Triad is the combination of confidentiality, integrity, and availability. Confidentiality is the concept of the measures used to ensure the protection of the secrecy of data, information, or resources. Integrity is the concept of protecting the reliability and correctness of data. Availability is the concept that authorized subjects are granted timely and uninterrupted access to objects. The term *CIA Triad* is used to indicate the three key components of a security solution.
2. The requirements of accounting are identification, authentication, authorization, and auditing. Each of these components needs to be legally supportable to truly hold someone accountable for their actions.
3. The six security roles are senior manager, security professional, asset owner, custodian, operator/user, and auditor.
4. The four components of a security policy are policies, standards, guidelines, and procedures. Policies are broad security statements. Standards are definitions of hardware and software security compliance. Guidelines are used when there is not an appropriate procedure. Procedures are detailed step-by-step instructions for performing work tasks in a secure manner.

Chapter 2: Personnel Security and Risk Management Concepts

1. Possible answers include job descriptions, principle of least privilege, separation of duties, job responsibilities, job rotation/cross-training, performance reviews, background checks, job action warnings, awareness, training, job training, exit interviews/terminations, nondisclosure agreements, employment agreements, privacy declaration, and acceptable use policies.
2. The formulas and values for quantitative risk assessment are as follows:

   AV = $

   EF = % loss

   SLE = AV * EF

   ARO = # / yr

   ALE = SLE * ARO or AV * EF * ARO

   Cost/benefit = (ALE1 – ALE2) – ACS
3. The Delphi technique is an anonymous feedback-and-response process used to enable a group to reach an anonymous consensus. Its primary purpose is to elicit honest and uninfluenced responses from all participants. The participants are usually gathered into a single meeting room. For each request for feedback, each participant writes down their response on paper or through digital messaging services anonymously. The results are compiled and presented to the group for evaluation. The process is repeated until a consensus is reached. The goal or purpose of the Delphi technique is to facilitate the evaluation of ideas, concepts, and solutions on their own merit without the discrimination that often occurs based on who the idea comes from.

4. Risk assessment often involves a hybrid approach using both quantitative and qualitative methods. A purely quantitative analysis is not possible; not all elements and aspects of the analysis can be quantified because some are qualitative, some are subjective, and some are intangible. Since a purely quantitative risk assessment is not possible, balancing the results of a quantitative analysis is essential. The method of combining quantitative and qualitative analyses into a final assessment of organizational risk is known as hybrid assessment or hybrid analysis.
5. The common social engineering principles are authority, intimidation, consensus, scarcity, familiarity, trust, and urgency.
6. Possible answers include eliciting information, pretexting, prepending, phishing, spear phishing, business email compromise (BEC), whaling, smishing, vishing, spam, shoulder surfing, invoice scams, hoaxes, impersonation, masquerading, tailgating, piggybacking, baiting, dumpster diving, identity fraud, typosquatting, influence campaigns, hybrid warfare, and social media abuse.

Chapter 3: Business Continuity Planning

1. Many federal, state, and local laws or regulations require businesses to implement BCP provisions. Including legal representation on your BCP team helps ensure that you remain compliant with laws, regulations, and contractual obligations.
2. The informal “seat-of-the-pants” approach is an excuse used by individuals who do not want to invest time and money in the proper creation of a BCP. This can lead to a catastrophe when a firmly laid plan isn't in place to guide the response during a stressful emergency situation.
3. Quantitative risk assessment involves using numbers and formulas to make a decision. Qualitative risk assessment includes expertise instead of numeric measures, such as emotions, investor/consumer confidence, and workforce stability.
4. The BCP training plan should include a plan overview briefing for all employees and specific training for individuals with direct or indirect involvement. In addition, backup personnel should be trained for each key BCP role.
5. The four steps of the BCP process are project scope and planning, business impact analysis, continuity planning, and plan approval and implementation.

Chapter 4: Laws, Regulations, and Compliance

1. The two key mechanisms used to facilitate information transfers are standard contractual clauses (SCCs) and binding corporate rules (BCRs). In the past, organizations could rely on the EU/US Privacy Shield safe harbor agreement, but this agreement was deemed invalid by the Court of Justice of the European Union (CJEU).
2. Some common questions that organizations should ask about outsourced service providers are as follows:
    - What types of sensitive information are stored, processed, or transmitted by the vendor?
    - What controls are in place to protect the organization's information?
    - How is your organization's information segregated from that of other clients?
    - If encryption is relied on as a security control, what encryption algorithms and key lengths are used? How is key management handled?
    - What types of security audits does the vendor perform, and what access does the client have to those audits?
    - Does the vendor rely on any other third parties to store, process, or transmit data? How do the provisions of the contract related to security extend to those third parties?
    - Where will data storage, processing, and transmission take place? If outside the home country of the client and/or vendor, what implications does that have?
    - What is the vendor's incident response process and when will clients be notified of a potential security breach?
    - What provisions are in place to ensure the ongoing integrity and availability of client data?

3. Some common steps that employers can take to notify employees of monitoring include clauses in employment contracts that state the employee should have no expectation of privacy while using corporate equipment, similar written statements in corporate acceptable use and privacy policies, logon banners warning that all communications are subject to monitoring, and labels on computers and telephones warning of monitoring.

Chapter 5: Protecting Security of Assets

1. Sensitive data is any data that isn't public. It includes personally identifiable information (PII), protected health information (PHI), proprietary data, and any other data that an organization needs to protect. PII is any information that can be used to identify an individual.
2. End of life (EOL) identifies the date when a vendor plans to stop selling and producing a product. End of support (EOS) identifies the date when a vendor plans to stop supporting a product. Organizations should replace products before the EOS date.
3. Organizations use pseudonymization when they want to create a dataset that they can transfer to others. The new dataset doesn't hold any privacy-related data. However, the organization still holds the mapping of the pseudonyms and the original data and can reverse the process. Organizations that process credit card data use tokenization. A third party holds the mapping of the token and the credit card data, but the organization doesn't need to maintain the credit card data. Organizations use anonymization to remove all privacy data from a dataset.
4. Tailoring refers to modifying a list of controls to ensure they align with the mission of the organization. Tailoring includes scoping. Scoping refers to reviewing a list of baseline security controls and selecting only those controls that apply to the IT systems you're trying to protect.

Chapter 6: Cryptography and Symmetric Key Algorithms

1. The major obstacle to the widespread adoption of one-time pad cryptosystems is the difficulty in creating and distributing the very lengthy keys on which the algorithm depends.
2. The first step in encrypting the message, “I will pass the CISSP exam and become certified next month” using columnar transposition requires the assignment of numeric column values to the letters of the secret keyword SECURE:

```
S E C U R E
5 2 1 6 4 3
```

   Next, the letters of the message, “I will pass the CISSP exam and become certified next month” are written in order underneath the letters of the keyword:

```
S E C U R E
5 2 1 6 4 3
I W I L L P
A S S T H E
C I S S P E
X A M A N D
B E C O M E
C E R T I F
I E D N E X
T M O N T H
```

   Finally, the sender enciphers the message by reading down each column; the order in which the columns are read corresponds to the numbers assigned in the first step. This produces the following ciphertext:

```
I S S M C R D O W S I A E E E M P E E D E F X H L H P N M I
E T I A C X B C I T L T S A O T N N
```

3. This message is decrypted by using the following function:

```
P = (C - 3) mod 26
C: F R Q J U D W X O D W L R Q V B R X J R W L W
```

P: C O N G R A T U L A T I O N S Y O U G O T I T

The hidden message is “CongratulationsYouGotIt.”
Congratulations, you got it!

Chapter 7: PKI and Cryptographic Applications

1. Bob should encrypt the message using Alice's public key and then transmit the encrypted message to Alice.
2. Alice should decrypt the message using her private key.
3. Bob should generate a message digest from the plaintext message using a hash function. He should then encrypt the message digest using his own private key to create the digital signature. Finally, he should append the digital signature to the message and transmit it to Alice.
4. Alice should decrypt the digital signature in Bob's message using Bob's public key. She should then create a message digest from the plaintext message using the same hashing algorithm Bob used to create the digital signature. Finally, she should compare the two message digests. If they are identical, Alice has assurance of message integrity. Alice should then make sure Bob's certificate is valid and issued from a trusted CA.

Chapter 8: Principles of Security Models, Design, and Capabilities

1. Security models include state machine (establishes the concept of a perfectly secure system), information flow (controls movement of data), noninterference (actions of subjects at one level do not affect the system state or actions of subjects at other levels), take-grant (control passage of rights to subjects), access control matrix (provides a perspective on access of multiple subjects across multiple objects), Bell–LaPadula (protects confidentiality), Biba (protects integrity), Clark–Wilson (protects integrity), and Brewer and Nash (avoids conflicts of interest).
2. The primary components of the trusted computing base (TCB) are the hardware and software elements used to enforce the security policy (these elements are called the TCB), the security perimeter distinguishing and separating TCB components from non-TCB components, and the reference monitor that serves as an access control device across the security perimeter.
3. The two primary rules of Bell–LaPadula are the simple rule of no read-up and the star rule of no write-down. The two rules of Biba are the simple rule of no read-down and the star rule of no write-up.
4. An open system is one with published APIs that allows third parties to develop products to interact with it. A closed system is one that is proprietary with no third-party product support. Open-source is a coding stance that allows others to view the source code of a program. Closed-source is an opposing coding stance that keeps source code confidential.
5. There are at least eight design principles listed in this chapter: objects and subjects, open and closed systems, secure defaults, fail securely, keep it simple, zero trust (trust but verify), privacy by design, and Secure Access Service Edge (SASE). Please compare your descriptions to the text in each section under the heading “Secure Design Principles.”

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

1. An industrial control system (ICS) is a form of computer-management device that controls industrial processes and machines (aka operational technology). There are several forms of ICS, including programmable logic controllers (PLCs), distributed control systems (DCSs), and supervisory control and data acquisition (SCADA). PLC units are effectively single-purpose or focused-purpose digital computers. They are typically deployed for the management and automation of various industrial electromechanical operations. DCS units are typically found in industrial process plants where the need to gather data and implement control over a large-scale environment from a single location is essential. A SCADA system can operate as a stand-alone device, can be networked together with other SCADA systems, or can be networked with traditional IT systems. A DCS focuses on processes and is state driven, whereas SCADA focuses on data gathering and is event driven. A DCS is used to control processes using a network of sensors, controllers, actuators, and operator terminals and is able to carry out advanced process control techniques. DCS is more suited to operating on a limited scale, whereas SCADA is suitable for managing systems over large geographic areas.
2. The three pairs of aspects or features used to describe storage are primary versus secondary, volatile versus nonvolatile, and random versus sequential.
3. Some vulnerabilities found in distributed architecture include sensitive data found on desktops/terminals/laptops, lack of security understanding among users, greater risk of physical component theft, compromise of a client leading to the compromise of the whole network, greater risk from malware because of user-installed software and removable media, and data on clients less likely to be included in backups.

4. Examples of server-based technologies include large-scale parallel data systems, SMP, AMP, MPP, grid computing, peer-to-peer computing, ICS, PLC, DCS, SCADA, DCE, IoT, IIoT, microservices, SOA, IaC, SDV, virtualized systems (virtual software, virtual networking, SDN), SDx, SDS, SDDC, VDI, VMI, SDV, containerization, and serverless architecture.
5. There were over 20 potential on-device security features mentioned in this chapter; any seven of the following would be correct: device authentication, full-device encryption, remote wiping, device lockout, screen locks, GPS and location services management, content management, application control, push notification management, third-party application store control, storage segmentation, asset tracking, removable storage, managing connection methods, deactivating unused features, rooting/jailbreaking, sideloading, custom firmware, carrier unlocking, firmware OTA updates, credential management, and text messaging security. Note that MDM/UEM is not an on-device security feature but an external tool used to configure those features. There are four main mobile device deployment models: BYOD, CYOD, COPE, and COMS/COBO. VDI and VMI are alternative means to grant users access to company resources, but they are not mobile device deployment models. There were over a dozen potential issues that should be addressed on a mobile device deployment policy mentioned in this chapter, and any seven of the following would be correct: data ownership, support ownership, patch and update management, security product management, forensics, privacy, architecture/infrastructure considerations, legal concerns, acceptable use policies, onboard cameras/video, recording microphone, tethering and hotspots, and contactless payment methods.

Chapter 10: Physical Security Requirements

1. A fence is an excellent perimeter safeguard that can help to deter casual trespassing. Moderately secure installations work when the fence is 6 to 8 feet tall and will typically be cyclone (also known as chain link) fencing with the upper surface twisted or barbed to deter casual climbers. More secure installations usually opt for fence heights over 8 feet and often include multiple strands of barbed or razor wire strung above the chain link fabric to further deter climbers.
2. Halon is an effective fire suppression compound (it starves a fire of oxygen by disrupting the chemical reaction of combustion), but it degrades into toxic gases at 900 degrees Fahrenheit. Also, it is not environmentally friendly (it is an ozone-depleting substance). The 1989 Montreal Protocol initiated the termination of the manufacturing of ozone-depleting substances, which includes halon. In 1994, the EPA banned the manufacture of halon in the United States and banned importing halon into the country. However, according to the Montreal Protocol, you can obtain halon by contacting a halon recycling facility. The EPA seeks to exhaust existing stocks of halon to take this substance out of circulation, there are still significant domestic stockpiles of halon.
3. Any time water is used to respond to fire, flame, or smoke, water damage becomes a serious concern, particularly when water is released in areas where electrical equipment is in use. Not only can computers and other electrical gear be damaged or destroyed by water, but many forms of storage media can also become damaged or unusable. Also, firefighters often use axes to break down doors or cut through walls to reach them as quickly as possible when seeking hot spots to extinguish. This, too, poses the potential for physical damage to or destruction of devices and/or wiring that may also be in the vicinity.
4. A proximity device can be a passive device, a field-powered device, or a transponder. The proximity device is worn or held by the authorized bearer. When it passes near a proximity

reader, the reader device is able to determine who the bearer is and whether they have authorized access. The passive proximity device has no active electronics; it is just a small magnet with specific properties (like antitheft devices commonly found in or on retail product packaging). A passive device reflects or otherwise alters the electromagnetic (EM) field generated by the reader device. This alteration is detected by the reader device, which triggers the alarm, records a log event, or sends a notification. A field-powered proximity device has electronics that activate when the device enters the EM field that the reader generates. Such devices generate electricity from an EM field to power themselves (such as card readers that only require the access card to be waved within inches of the reader to unlock doors). This is effectively the concept of radio-frequency identification (RFID). A transponder proximity device is self-powered and transmits a signal received by the reader. This can occur consistently or only at the press of a button (like a garage door opener or car alarm key fob). Such devices may have batteries, capacitors, or even be solar-powered.

Chapter 11: Secure Network Architecture and Components

1. Application (7), Presentation (6), Session (5), Transport (4), Network (3), Data Link (2), and Physical (1).
2. Problems with cabling and their countermeasures include attenuation (use repeaters or don't violate distance recommendations), using the wrong category of cable (check the cable specifications against throughput requirements, and err on the side of caution), crosstalk (use shielded cables, place cables in separate conduits, or use cables of different twists per inch), interference (use cable shielding, use cables with higher twists per inch, or switch to fiber-optic cables), and eavesdropping (maintain physical security over all cable runs or switch to fiber-optic cables).
3. Some of the frequency spectrum-use technologies are spread spectrum, Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), and Orthogonal Frequency-Division Multiplexing (OFDM).
4. Methods used to secure 802.11 wireless networking include updating firmware; changing the default administrator password to something unique and complex; enabling WPA2 or WPA3 encryption; disabling the SSID broadcast; changing the SSID to something unique; changing the wireless MAC address; enabling MAC filtering; considering the use of static IPs or using DHCP with reservations; treating wireless as remote; separating WAPs from the LAN with firewalls; monitoring all wireless client activity with an IDS; deploying a wireless intrusion detection system (WIDS) and a wireless intrusion prevention system (WIPS); considering requiring wireless clients to connect with a VPN to gain LAN access; implementing a captive portal; and tracking/logging all wireless activities and events.
5. The applications and ports listed in this chapter you could have selected include: Telnet, TCP Port 23; File Transfer Protocol (FTP), TCP Ports 20 (Active Data Connection)/Ephemeral

(Passive Data Connection) and 21 (Control Connection); Simple Mail Transfer Protocol (SMTP), TCP Port 25; SMTPS STARTTLS, TCP Port 587, SMTPS Implicit, TCP Port 465; Post Office Protocol (POP3), TCP Port 110; POPS, TCP Port 995; Internet Message Access Protocol (IMAP), TCP Port 143; IMAPS, TCP Port 993; Dynamic Host Configuration Protocol (DHCP), UDP Ports 67 and 68; Hypertext Transfer Protocol (HTTP), TCP Port 80; HTTPS with Transport Layer Security (TLS), TCP Port 443; Line Print Daemon (LPD), TCP Port 515; Network File System (NFS), TCP Port 2049; Simple Network Management Protocol (SNMP), UDP Port 161 (UDP Port 162 for Trap Messages); and Domain Name System (DNS), TCP/UDP 53.

Chapter 12: Secure Communications and Network Attacks

1. Transport mode links or VPNs are anchored or end at the individual hosts connected together. Let's use IPSec as an example. In transport mode, IPSec provides encryption protection for just the payload and leaves the original message header intact. This type of VPN is also known as a host-to-host VPN or an end-to-end encrypted VPN, since the communication remains encrypted while it is in transit between the connected hosts. Tunnel mode links or VPNs are anchored or end at VPN devices on the boundaries of the connected networks (or one remote device). In tunnel mode, IPSec provides encryption protection for both the payload and message header by encapsulating the entire original LAN protocol packet and adding its own temporary IPSec header. Tunnel mode VPNs can be used to connect two networks across the Internet (aka site-to-site VPN) or to allow distant clients to connect into an office local area network (LAN) across the Internet (aka remote access VPN).
2. Network address translation (NAT) allows the identity of internal systems to be hidden from external entities. Often NAT is used to translate between RFC 1918 private IP addresses and leased public addresses. NAT serves as a one-way firewall because it allows only inbound traffic that is a response to a previous internal query. NAT also allows a few leased public addresses to be used to grant internet connectivity to a larger number of internal systems.
3. Circuit switching is usually associated with physical connections. The link itself is physically established and then dismantled for the communication. Circuit switching offers known fixed delays, supports constant traffic, is connection oriented, is sensitive only to the loss of the connection rather than the communication, and is most often used for voice transmissions. Packet switching is usually associated with logical connections because the link is just a logically defined path among possible

paths. Within a packet-switching system, each system or link can be employed simultaneously by other circuits. Packet switching divides the communication into segments, and each segment traverses the circuit to the destination. Packet switching has variable delays because each segment could take a unique path, is usually employed for bursty traffic, is not physically connection oriented but often uses virtual circuits, is sensitive to the loss of data, and is used for any form of communication.

4. Email is inherently insecure because it is primarily a plaintext communication medium and employs nonencrypted transmission protocols. This allows email to be easily spoofed, spammed, flooded, eavesdropped on, interfered with, and hijacked. Defenses against these issues primarily include having stronger authentication requirements and using encryption to protect the content while in transit.

5. The RFC 1918 private IP address ranges are as follows: 10.0.0.0–10.255.255.255 (a full Class A range); 172.16.0.0–172.31.255.255 (16 Class B ranges); and 192.168.0.0–192.168.255.255 (256 Class C ranges). APIPA assigns each failed DHCP client with an IP address from the range of 169.254.0.1 to 169.254.255.254 along with the default Class B subnet mask of 255.255.0.0. Technically, the entire 127.0.0.0/8 network is reserved for loopback use in IPv4. However, only the 127.0.0.1 address is widely used.

6. Many facts about VLANs are included in this chapter. Answers can include any of the following options. A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs can be defined/assigned/created based on ports, device MAC address, IP subnetting, specified protocols, or authentication. VLANs are used for traffic management because they are a form of network segmentation. VLAN routing can be provided either by an external router or by the switch's internal software (one reason for the terms *L3 switch* and *multilayer switch*). VLANs control and restrict broadcast traffic and reduce a network's vulnerability to sniffers because a switch treats each VLAN as a separate network

division. The members of a private VLAN or a port-isolated VLAN can interact only with one another and over the predetermined exit port or uplink port. The trunk link allows the switches to talk to each other directly, direct traffic between hosts, and stretch VLAN definitions across multiple physical switches.

Chapter 13: Managing Identity and Authentication

1. Physical access controls are anything you can touch. They include perimeter security controls (such as fences and gates) and environmental controls such as heating, ventilation, and air-conditioning (HVAC) systems. Logical access controls are also known as technical controls. They include authentication, authorization, and permission controls.
2. Identification occurs when a subject claims an identity, such as with a username. Authentication occurs when the subject provides information to verify the claimed identity is the subject's identity. For example, a user provides the correct password matched to the username. Authorization is the process of granting the subject rights and permissions based on the subject's proven identity. Accounting is accomplished by logging subjects' actions and is reliable only if the identification and authentication processes are strong and secure.
3. The three primary authentication factor types are something you know, something you have, and something you are, also known as Type 1, Type 2, and Type 3, respectively. Something you know is a memorized secret such as a password or PIN. Something you have includes devices that a person can touch and hold, such as a smartcard or hardware authenticator. Something you are uses biometric methods such as fingerprints or facial identification.
4. Federated identity management (FIM) systems allow single sign-on (SSO) to be extended beyond a single organization. SSO allows users to authenticate once and access multiple resources without authenticating again. SAML is a common language used to exchange federated identity information between organizations.
5. Organizations use provisioning and onboarding processes when hiring employees and deprovisioning and offboarding processes when employees leave.

Chapter 14: Controlling and Monitoring Access

1. The primary difference between discretionary and nondiscretionary access control models is in how they are controlled and managed. Administrators centrally administer nondiscretionary access controls. DAC models allow owners to make their own changes, and their changes don't affect other parts of the environment.
2. Some common standards used to provide SSO capabilities on the Internet are Security Assertion Markup Language (SAML), OAuth, and OpenID Connect (OIDC).
3. The PowerShell cmdlet that allows you to run PowerShell commands indirectly is `Invoke-Expression`. The following command shows how to run it, assuming you have a PowerShell script named `hello.ps1` in the current directory:

   ```
   powershell.exe "& {Get-Content .\hello.ps1 | Invoke-
   Expression}
   ```

   If you want to see this in action, create the `hello.ps1` file with the following line:

   ```
   Write-Host 'Hello, World'
   ```

4. Mimikatz is a popular tool used in privilege escalation attacks, including pass the hash and Kerberos exploitation attacks. PsExec, one of the tools in the Sysinternals process utilities (PsTools), is another tool often used in these attacks.

Chapter 15: Security Assessment and Testing

1. TCP SYN scanning sends a single packet to each scanned port with the SYN flag set. This indicates a request to open a new connection. If the scanner receives a response that has the SYN and ACK flags set, this indicates that the system is moving to the second phase in the three-way TCP handshake and that the port is open. TCP SYN scanning is also known as “half-open” scanning. TCP connect scanning opens a full connection to the remote system on the specified port. This scan type is used when the user running the scan does not have the necessary permissions to run a half-open scan.
2. The five possible port status values returned by Nmap are as follows:
    - *Open*: The port is open on the remote system and there is an application that is actively accepting connections on that port.
    - *Closed*: The port is accessible on the remote system, meaning that the firewall is allowing access, but there is no application accepting connections on that port.
    - *Filtered*: Nmap is unable to determine whether a port is open or closed because a firewall is interfering with the connection attempt.
    - *Unfiltered*: The port is accessible, but Nmap cannot determine whether it is open or closed. It is unfiltered because the port is exposed to the packet probes sent by Nmap, but no conclusive evidence can determine the port's status.
    - *Open | Filtered*: Nmap cannot establish whether the port is open or filtered. This state occurs when a port does not respond to Nmap's probes, which could be due to packet filtering preventing Nmap's requests from reaching the

port, or the port is open but designed not to respond to the probes used by Nmap.

3. Static software testing techniques, such as code reviews, evaluate the security of software without running it by analyzing either the source code or the compiled application. Dynamic testing evaluates the security of software in a runtime environment and is often the only option for organizations deploying applications written by someone else.
4. Mutation (dumb) fuzzing takes previous input values from actual operation of the software and manipulates (or mutates) it to create fuzzed input. It might alter the characters of the content, append strings to the end of the content, or perform other data manipulation techniques.

   Generational (intelligent) fuzzing develops data models and creates new fuzzed input based on an understanding of the types of data used by the program.

Chapter 16: Managing Security Operations

1. Need-to-know focuses on permissions and the ability to access information, whereas the least privilege principle focuses on privileges. Privileges include both rights and permissions. Both limit the access of users and subjects to only what they need. Following these principles prevents and limits the scope of security incidents.
2. Monitoring the assignment and usage of special privileges detects when individuals are granted higher privileges, such as when they are added to an Administrator account. It can detect when unauthorized entities are granted higher privileges. Monitoring the usage of special privileges detects when entities are using higher privileges, such as creating unauthorized accounts, accessing or deleting logs, and creating automated tasks. This monitoring can detect potential malicious insiders and remote attackers.
3. The three primary cloud-based service models are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). The cloud service provider (CSP) provides the most maintenance and security services with SaaS, less with PaaS, and the least with IaaS. While NIST SP 800-145 provides these definitions, CSPs sometimes use their own terms and definitions in marketing materials.
4. Change management processes help prevent outages by ensuring that proposed changes are reviewed, approved, and tested before being deployed. They also ensure that changes are documented.

Chapter 17: Preventing and Responding to Incidents

1. An incident is any event that has a negative effect on the confidentiality, integrity, or availability of an organization's assets.
2. Incident management steps listed in the CISSP Security Operations domain are detection, response, mitigation, reporting, recovery, remediation, and lessons learned.
3. Intrusion detection systems are described as host-based or network-based, knowledge-based or behavior-based, and passive or active. Host-based IDSs examine events on individual computers in great detail, including file activities, accesses, and processes. Network-based IDSs examine general network events and anomalies through traffic evaluation. A knowledge-based IDS uses a database of known attacks to detect intrusions. A behavior-based IDS starts with a baseline of normal activity and measures network activity against the baseline to identify abnormal activity. A passive response will log the activity and often provide a notification. An active response directly responds to the intrusion to stop or block the attack.
4. A SIEM system collects log entries from multiple sources in a centralized application. It can accept data from dissimilar devices and correlate and aggregate all of the data into useful information. It can also be configured to send alerts in real time to specific items of interest.
5. Security orchestration, automation, and response (SOAR) refers to a group of technologies that automatically respond to some incidents. This reduces the workload on administrators.

Chapter 18: Disaster Recovery Planning

1. Businesses have three main concerns when considering adopting a mutual assistance agreement. First, the nature of an MAA often necessitates that the businesses be located in close geographical proximity. However, this requirement also increases the risk that the two businesses will fall victim to the same threat. Second, MAAs are difficult to enforce in the middle of a crisis. If one of the organizations is affected by a disaster and the other isn't, the organization not affected could back out at the last minute, leaving the other organization out of luck. Finally, confidentiality concerns (both legal and business related) often prevent businesses from trusting others with their sensitive operational data.
2. There are six main types of disaster recovery tests:
    - Read-throughs involve the distribution of recovery checklists to disaster recovery personnel for review.
    - Tabletops involve the members of the disaster recovery team gathering in a large conference room and role-playing a disaster scenario.
    - Walk-through exercises include taking physical actions or at least considering their impact on the exercise.
    - Simulation tests are more comprehensive and may impact one or more noncritical business units of the organization.
    - Parallel tests involve relocating personnel to the alternate site and commencing operations there.
    - Full-interruption tests involve relocating personnel to the alternate site and shutting down operations at the primary site.
3. Full backups create a copy of all data stored on a server. Incremental backups create copies of all files modified since the last full or incremental backup. Differential backups create copies of all files modified since the last full backup without

regard to any previous differential or incremental backups that may have taken place.

4. Cloud computing influences disaster recovery programs in two major ways. First, the cloud provides excellent opportunities for disaster recovery operations, offering on-demand access to technology resources. Second, organizations using the cloud must ensure that they implement disaster recovery capabilities within their cloud environment using controls offered by the cloud service provider, built internally, or offered by third parties.

Chapter 19: Investigations and Ethics

1. The major categories of computer crime are military/intelligence attacks, business attacks, financial attacks, terrorist attacks, grudge attacks, thrill attacks, and hacktivist attacks.
2. Thrill attacks are motivated by individuals seeking to achieve the "high" associated with successfully breaking into a computer system.
3. Interviews are conducted with the intention of gathering information from individuals to assist with your investigation. Interrogations are conducted with the intent of gathering evidence from suspects to be used in a criminal prosecution.
4. To be admissible, evidence must be reliable, competent, and material to the case.

Chapter 20: Software Development Security

1. The primary key uniquely identifies each row in the table. For example, an employee identification number might be the primary key for a table containing information about employees.
2. Polyinstantiation is a database security technique that appears to permit the insertion of multiple rows sharing the same uniquely identifying information.
3. Supervised and unsupervised machine learning techniques both use training datasets to develop models, but they differ in the nature and use of those training datasets. In supervised techniques, the instances use labeled data that contains the correct answers that the model should learn how to apply to future instances. In unsupervised techniques, the data is not labeled and the algorithm is asked to identify those labels as part of the learning process.

Chapter 21: Malicious Code and Application Attacks

1. Viruses and worms both travel from system to system attempting to deliver their malicious payloads to as many machines as possible. However, viruses require human intervention, such as sharing a file, network resource, or email message, to propagate. Worms, on the other hand, seek out vulnerabilities and spread from system to system under their own power, thereby greatly magnifying their reproductive capability, especially in a well-connected network.
2. If possible, antivirus software may try to disinfect an infected file, removing the virus's malicious code. If that fails, it might either quarantine the file for manual review or automatically delete it to prevent further infection.
3. Data integrity assurance packages like Tripwire compute hash values for each file stored on a protected system. If a file infector virus strikes the system, this would result in a change in the affected file's hash value and would therefore trigger a file integrity alert.
4. Defending against SQL injection vulnerabilities requires a defense-in-depth approach. It may include the use of whitelisting and/or blacklisting input validation, stored procedures/parameterized queries, web application security scans, web application firewalls, and other controls.